MONTANA CHEMICAL DEPENDENCY CENTER POLICY AND PROCEDURE MANUAL

Policy Subject: Workstation & Portable Computer Security	
Policy Number: CUP 12	**Standards/Statutes: ARM 37.27.120**
Effective Date: 01/01/02	**Page 1 of 2**

PURPOSE:
The Montana Chemical Dependency Center is responsible for establishing minimum-security standards and policies, including the physical security of the central and backup computer facilities. It is of extreme importance that workstation and portable computer security be maintained, especially with the expansion of the network and the number of people having access to the network. This policy is intended to set minimum standards for the security of the workstations and portable computers owned by the State of Montana.

POLICY:
This policy shall govern all entities within the scope of the Montana Chemical Dependency Center.

PROCEDURE:
Workstations and portable computers will be kept out of sight and covered when stored in a vehicle. A tag that includes the name, address and phone number of the agency must be attached to the outside of all portable computers. Workstations and portable computers will be inventoried annually with discrepancies reported appropriately.
Each user is responsible for maintaining the security of their own workstation and/or portable computer and for following the security requirements implemented by the Montana Chemical Dependency Center.

Users will not use another employee's User ID and will not have more than one simultaneous connection on the network. All exceptions to this rule will be documented.

Workstations with unattended processes running on them must have some type of screen saver with password protection or keyboard locking program enabled on them.

Passwords must be at least 6 characters long and contain at least one numeric and one alphabetic character. Passwords must be changed at least every 60 days. Passwords must not be reused for at least 4 cycles. Passwords must not be written down where they can be found by unauthorized personnel and should not be shared with other individuals. Logon IDs will be suspended if unused for over 90 days.

If a user changes work positions in an agency, their access rights must be reviewed and changed to match the new job position. Power on or system passwords should be used on workstations that are in highly accessible areas and on portable computers. Power on passwords should be provided to the Information Systems Technician and kept in a secure place.

Workstations and portable computers will be kept out of sight and covered when stored in a vehicle. Any software installed that uses script files must not contain a user ID or password for the State's computer system. Portable computers MUST be transported as carry on luggage when traveling by plane or bus. If highly sensitive information is stored on a portable computer, the data should be encrypted.

Passwords should not be obvious or easily guessed (User ID, user's name, address, birth date, child's name, spouse's name, etc).

User rights should be periodically reviewed.

Revisions:_____

Prepared By: Rona McOmber Information System Technician 10/30/01
Name Title Date

Approved By:_____ 11/06/01
David J. Peshek, Administrator